

# MISSOURI DEPARTMENT OF MENTAL HEALTH



DEPARTMENT  
OPERATING  
REGULATION  
NUMBER

DOR  
8.340

Dorn Schuffman, Department Director

CHAPTER Regulatory Compliance	SUBCHAPTER HIPAA Regulations	EFFECTIVE DATE 09-01-03	NUMBER OF PAGES 2	PAGE NUMBER 1 of 2
SUBJECT Use of Email Containing PHI		AUTHORITY 630.050 RSMo		History See Below
PERSON RESPONSIBLE Director of Information Systems			Sunset 7/1/07	

*Purpose: The policy of the Missouri Department of Mental Health is to secure consumer's protected health information (PHI) in compliance with federal law and federal regulations at 45 CFR Sections 164.530(c)(1) and (2), and 42 CFR Part 2. This DOR addresses using Email containing unencrypted PHI.*

*Application: Applies to entire Department of Mental Health, its facilities and workforce.*

## (1) Contents

- (A) Definitions
- (B) Procedures for using Email
- (C) DOR control
- (D) Sanctions
- (E) Review Process

## (2) Definitions

(A) DMH Workforce – Includes employees, volunteers, contract workers, trainees, interns and other persons who are in a DMH facility or Central Office on a regular course of business. This shall include client workers employed by the DMH or any of its facilities.

(B) Chief Security Officer (Chief Security Officer) - Individual designated by the DMH to oversee all activities related to the development, implementation, maintenance of, and adherence to Department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

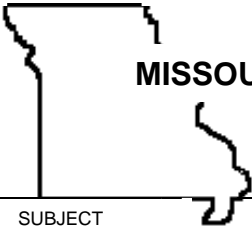
(C) Local Security Officer (LSO) – Individual designated by a facility CEO to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer.

(D) Email – The electronic transfer of information in the form of electronic notes and memorandum. Also includes the transfer of information between DMH staff and staff of other State agencies, providers, and other organizations with whom the DMH has a business relationship.

(E) Protected Health Information (PHI) – Individually identifiable health information.

(F) Microsoft Word – a business software program that serves as the Department's main word processing program.

(G) Microsoft Excel - a business software program that serves as the Department's main financial/spreadsheet program.



# MISSOURI DEPARTMENT OF MENTAL HEALTH

DORN SCHUFFMAN, DEPARTMENT DIRECTOR



DEPARTMENT  
OPERATING  
REGULATION  
NUMBER

DOR  
8.340

SUBJECT	EFFECTIVE DATE	NUMBER OF PAGES	
User Access to Electronic Data	09/01/03	2	2 of 2

(H) Microsoft Exchange – a business program that serves as the Department’s main Email program.

(I) DMH Global Address List – the list contained in Microsoft Exchange which contains the Email address of all DMH employees.

(3) Procedures for using Email. Until such time as the State of Missouri adopts a statewide encryption standard, the following Email procedures shall be followed.

(A) DMH staff are prohibited from sending Email that contains PHI to any State agency, provider, or other organizations with whom the DMH has a business relationship with the following exceptions:

1. Staff may password-protect Microsoft Word or Microsoft Excel documents containing PHI and attach those to Email. Staff shall use a unique password on every document sent;

2. Staff shall call or fax the recipient of the Email and let them know the password;

3. Staff shall not include the password within the contents of the Email; and

4. Staff shall also be diligent in not forwarding emails that contain PHI.

(B) If the State agency, provider, or other organizations with whom the DMH has a business relationship does not use Word or Excel, PHI may only be transmitted over the phone or by fax.

(C) Staff may continue to send Email containing PHI to persons on the DMH Global Address List. Persons who have the globe icon next to their names are not DMH employees; Email containing PHI shall not be transmitted to them.

(4) There shall be no facility policies pertaining to this topic. The Department Operating Regulations shall control.

(5) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.

(6) Review Process. The Chief Security Officer will periodically collect information from the Local Security Officers and the Email administrators for the purpose of providing feedback to the Director, Office of Information Systems and to the DMH Executive Team regarding trends and issues associated with compliance with this regulation.

*History: Emergency DOR effective June 1, 2003; expires November 30, 2003.  
Emergency DOR withdrawn and final DOR effective September 1, 2003.*